



March 5, 2008
Via ECFS Transmission

2600 Maitland Center Pkwy.
Suite 300
Maitland, FL 32751
P.O. Drawer 200
Winter Park, FL
32790-0200
Tel: 407-740-8575
Fax: 407-740-0613
www.tminc.com

Marlene H. Dortch, Commission Secretary
Office of the Secretary
Federal Communications Commission
445 – 12th Street, SW – Suite TW-A325
Washington, D.C. 20554

RE: EB Docket No. 06-36
CPNI Certification for City of Bristol, dba Bristol Virginia Utilities also dba BVU
OptiNet, dba BVUB, dba OptiNet, and also dba BVU

Dear Ms. Dortch:

In accordance with Federal Communications Commission's Public Notice of January 29, 2008, and pursuant to 47 C.F.R. § 64.2009(e), City of Bristol, dba Bristol Virginia Utilities also dba BVU OptiNet, dba BVUB, dba OptiNet, and also dba BVU hereby files its Certification of Customer Proprietary Network information (CPNI) for the year 2007 and supporting Statement. As directed by the Public Notice, please include this Certification in EB Docket No. 06-36.

Please contact me at 407-740-3006 or croesel@tminc.com if you have any questions about this filing.

Sincerely,

A handwritten signature in black ink, appearing to read "C. Roesel".

Carey Roesel
Consultant to City of Bristol,
dba Bristol Virginia Utilities

CR/gs
Enclosure

cc: Enforcement Bureau (*provided via ECFS website*)
Best Copy and Printing (*FCC@BCPIWEB.COM*)
tms: FCCx0801
File: BVU – FCC Certs/Orders

**ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE**

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for Calendar Year: 2007

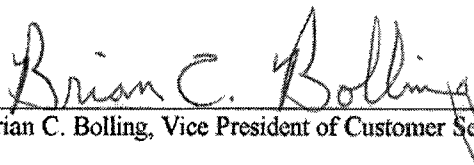
Name of company covered by this certification: City of Bristol dba Bristol Virginia Utilities

Name of signatory: Brian C. Bolling

Title of signatory: Vice President of Customer Service

I, Brian C. Bolling certify and state that:

1. I am the Vice President of Customer Service of City of Bristol dba Bristol Virginia Utilities ("BVU"), and, acting as an agent of the company, I have personal knowledge of BVU's operating procedures as they relate to CPNI, and the Rules and Regulations of the Federal Communications Commission regarding CPNI.
2. I hereby certify that, to the best of my knowledge, information and belief, BVU's operating procedures are adequate to ensure compliance with its CPNI obligations pursuant to Section 222 of the Communications Act of 1934, as amended, and the Commission's rules found at 47 CFR Subpart U.
3. Attached to this certification as Exhibit A is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.



Brian C. Bolling, Vice President of Customer Service

March 2, 2008

Date

Exhibit A
Statement of CPNI Procedures and Compliance

Statement of CPNI Procedures and Compliance

Use of CPNI

Bristol Virginia Utilities (“BVU”) does not use or permit access to CPNI to market any services outside of the total service approach as specified in 47 CFR §64.2005. If BVU elects to use CPNI in a manner that does require customer approval, it will follow the applicable rules set forth in 47 CFR Subpart U, including the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

PROTECTION OF CPNI

BVU has put into place processes to safeguard its customers’ CPNI/call detail information from improper use or disclosure by employees; and to discover and protect against attempts by third parties to gain unauthorized access to customer CPNI. BVU has a CPNI manual that covers disciplinary action and as part of the CPNI procedures employees sign a document that acknowledges potential disciplinary action. For example an excerpt states: *Violation by Company employees and agents of such CPNI requirements will lead to prompt disciplinary action (up to and including remedial training, reprimands, unfavorable performance reviews, probation, and termination), depending upon the circumstances of the violation (including the severity of the violation, whether the violation was a first time or repeat violation, whether appropriate guidance was sought or received from the CPNI Compliance Officer(s), and the extent to which the violation was or was not deliberate or malicious).*

IF COMPANY USES CPNI:

BVU ensures that all access to CPNI be approved by a supervisor with knowledge of the FCC's CPNI requirements. BVU has instituted training procedures and a corresponding disciplinary process to ensure that its personnel understand and comply with restrictions regarding the use and disclosure of, and access to, CPNI. All outbound marketing situations must be approved by the Compliance Officer and after approval the effort is documented. The Compliance Officer will maintain a record of each out-bound marketing activity or campaign, including:

- a. a description of the campaign;
- b. the specific CPNI that was used in the campaign;
- c. the date and purpose of the campaign;
- d. the name and relationship of any third party to which CPNI was disclosed or provided, or which was allowed to access CPNI; and
- e. what products and services were offered as part of the campaign.

DISCLOSURE OF CALL DETAIL OVER PHONE

BVU has instituted authentication procedures to safeguard the disclosure of call detail over the telephone. BVU's authentication procedures do not require the use of readily available biographical information or account information as defined by the FCC. BVU procedures allow that passwords can be designed in a manner that is privately significant and memorable to the customer (e.g., "pirates1971," "1836alamo," "\$beatles4"). However, passwords may NOT be based upon readily obtainable biographical information (e.g., the customer's name, mother's maiden name, social security number or date of birth) or account information (e.g., the customer's telephone number, address, account number, or amount of last bill). All customers are required to establish a password without the use of readily available biographical information or account information if they want to receive call detail over the telephone. If the appropriate password is not provided, BVU does not disclose call detail over the telephone.

BVU has established back-up authentication procedures for lost or stolen passwords that do not prompt the customer for readily available biographical information or account information. Company's back-up authentication procedure operates as follows (excerpt from the Company's CPNI manual):

b. The Company will establish a password (and a back-up customer authentication method if the customer loses or forgets his or her password) for each new customer at the time that the customer initiates service.

c. The Company will establish a new or replacement password (and a back-up customer authentication method if the customer loses or forgets his or her password) for existing customers desiring a password pursuant to the following procedure. The Company may periodically announce on its website, in its newsletter and/or in its billing materials that customers must have a password for security and privacy purposes in order to call the Company and obtain their call detail information over the telephone. The Company announcements will inform customers that they may obtain an initial or replacement password: (i) if they come in person to the Company's business office, produce a driver's license, passport or other government-issued identification verifying their identity, and correctly answer certain questions regarding their service and address; or (ii) if they call a specified Company telephone number from their "telephone number of record" (see definition above) and then wait at that number until a Company employee calls them back and obtains correct answers to certain questions regarding their service and address; or (iii) if they ask the Company to send a randomly-generated Personal Identification Number ("PIN") to their "telephone number of record" (see definition above) by voice, voicemail or text message or mail it to their "address of record" (see definition above), and then call the Company back and provide the correct PIN.

d. The Company's "back-up customer authentication method" will consist of a "shared secret" combination of two pre-selected questions by the Company and two pre-selected answers by the customer regarding two non-public

aspects of the customer's life that would not be known by a pretexter, hacker or other unauthorized entity. For example, such "shared secret" questions and answers might relate to the customer's favorite Holiday, color, song, book, movie, food, or sports team, or in what city were you born (unless such characteristic are a matter of public record or known by a significant number of people). If the customer claims to have lost or forgotten his or her password, but can correctly provide the pre-selected answers to the two pre-selected "shared secret" questions, the requested call detail information can be given to the customer over the telephone during the customer-initiated call.

Company has put into place procedures to notify customers whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed without revealing the changed information or sending the notification to the new account information. The notice may be provided by: (i) a Company call or voicemail to the customer's telephone number of record; (ii) a Company text message to the customer's telephone number of record; or (iii) a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

DISCLOSURE OF CPNI ONLINE

BVU has instituted authentication procedures to safeguard the disclosure of CPNI on-line. BVU's authentication procedures do not require the use of readily available biographical information or account information as defined by the FCC. Customers may have access to their billing via internet access to our secure server. Customer must establish a User ID and Password by entering a 5 digit secret number in conjunction with their account number. Unless the appropriate password is provided, BVU does not allow on-line access to CPNI.

BVU has established back-up authentication procedures for lost or stolen passwords that do not prompt the customer for readily available biographical information or account information. See above excerpt from BVU's CPNI manual.

Company has put into place procedures to notify customers whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed without revealing the changed information or sending the notification to the new account information. The notice may be provided by: (i) a Company call or voicemail to the customer's telephone number of record; (ii) a Company text message to the customer's telephone number of record; or (iii) a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

DISCLOSURE OF CPNI AT RETAIL LOCATIONS

Company discloses CPNI at its retail locations only if the customer has presented a valid photo ID matching his/her account information.

NOTIFICATION TO LAW ENFORCEMENT

Company has in place procedures to notify law enforcement in the event of a breach of customers' CPNI and to ensure that customers are not notified of the breach before the time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement.

BVU maintains records of all breaches discovered and notifications made to the USSS and the FBI, and to customers.

ACTIONS AGAINST DATA BROKERS

Company has not taken any actions against data brokers in the last year.

CUSTOMER COMPLAINTS ABOUT CPNI BREACHES

Company did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2007.

INFORMATION ABOUT PRETEXTERS

Company has developed the following information with respect to the processes pretexters are using to attempt to access CPNI and is taking the following steps to protect CPNI. BVU has stated the following in its CPNI manual:

In some unfortunate instances, pretexters have obtained CPNI from telephone company representatives who have cooperated for friendship, financial or other reasons. The Company will take any and all disciplinary, termination and/or remedial actions permitted by applicable federal and state employment law against any Company representative that is reasonably suspected to have cooperated knowingly and intentionally with a pretexter.

Pretexters may use a variety of tactics to try to fool telephone company representatives in order to get unauthorized and unlawful access to CPNI. Some of these tactics involve mock anger and bullying; others entail pleading and playing upon normal human emotions.